PUOLUSTUSHALLINNON RAKENNUSLAITOKSEN TURVALLISUUDENHALLINTAJÄRJESTELMÄ

10. Turvallisuusjohdon
koulutusohjelma
Teknillinen korkeakoulu
Koulutuskeskus Dipoli
Tutkielma 23.2.2010
Juha Ilkka

Juha Ilkka

SISÄLLYSLUETTELO

Juha Ilkka

1 TIIVISTELMÄ

Puolustushallinnon rakennuslaitoksen turvallisuustoiminnan perusteet on luotu jo ennen Rakennuslaitoksen perustamista, kun virasto on vuonna 1994 perustettu Puolustusministeriön rakennusosastosta ja puolustusvoiminen alueellista kiinteistöorganisaatiosta. Turvallisuus on sisällytetty osaksi toimintaprosesseja, sen sijaan että turvallisuustoiminnasta olisi tehty erillisiä prosesseja. Turvallisuusjohtaminen on aikaisemmin painottunut todella vahvasti operatiiviseen toimintaan, jonka varjopuolena on ollut suunnittelemattomuus ja osittainen ad-hoc -toiminta. Turvallisuudenhallintajärjestelmää ei ole formalisoitu, joka on näkynyt mm. hallitsemattomana kokonaisuutena. Tämän tutkimuksen tarkoituksena selvittää kolmen yleisen hallintamallin rakenteet (EK, OHSAS 18001 ja ISO 27001) ja selvittää kuinka niitä voidaan hyödyntää Rakennuslaitoksen turvallisuudenhallintajärjestelmässä. Rakennuslaitoksen turvallisuuteen vaikuttavat ulkopuoliset tekijät ovat Suomen laki, puolustusministeriön turvallisuustoiminnan strategia, puolustusvoimien turvallisuussopimus ja valtionhallinnon turvallisuuskriteeristöt (kansallinen turvallisuusauditointikriteeristö, tietoturvatasot sekä jatkuvuuden hallinnan ja tiedon turvaamisen vaatimukset). Yleisistä malleista mikään ei sellaisenaan sovellus Rakennuslaitoksen turvallisuudenhallintajärjestelmän malliksi. EK:n malli on kattava, mutta rakenteeseen ja itse toiminnan vaatimuksia ei kuvata juuri ollenkaan. OHSAS 18001 on ensisijaisesti tarkoitettu työterveyden ja työturvallisuuden johtamiseen. Sellaisenaan se ei toimi kokonaisvaltaisen turvallisuusjohtamisen malliksi. Viitekehystä voidaan kuitenkin hyödyntää Rakennuslaitoksen työterveyden ja työturvallisuuden hallintaan. ISO 27001 on tietoturvallisuudenhallintajärjestelmä, jossa huomioidaan iso osa kokonaisvaltaisesta turvallisuudenhallinnasta. Kuten OHSAS 18001, myös ISO 27001 perustuu PDCA (Plan-Do-Check-Act) -sykliin. ISO 27001 ei myöskään ole tarpeeksi kattava malli, joten lopputuloksena on näiden kolmen mallin synteesi. EK:n mallista on otettu turvallisuuden osa-alueet ja OHSAS 18001 sekä ISO 27001 –standardeista on otettu hallintajärjestelmän rakenne. Toiminnalle asetettavat kriteerit tulevat valtionhallinnon kriteereistä. Turvallisuudenhallintajärjestelmässä keskeiset kehityskohteet ovat turvallisuusvaatimusten kirjaaminen laitoksen laatujärjestelmään siten, että ne ovat sisäisen valvonnan auditoitavissa. Turvallisuuteen vaikuttavien asiakirjojen rakennetta tulee keventää niin, että ylätasolla on Puolustusministeriön turvallisuustoiminnan strategia jonka alla operatiivista puolta ohjaa Rakennuslaitoksen turvallisuuspolitiikka. Politiikkaan on sisällytetty kaikki osa-alueet kuten riskienhallinta, tietoturva ja tietosuoja. Politiikan vaatimukset jalkautetaan käytäntöön turvallisuuskäytännöillä ja toimintamalleilla. Alimmalla tasolla on yksittäiset ohjeet esim. tiedostojen salaamiseen. Tietoturvallisuudella ei saa olla omaa hallintajärjestelmää vaan se pitää integroida osaksi turvallisuudenhallintajärjestelmää.

2 JOHDANTO

2.1 Tutkimuksen tausta

Puolustushallinnon rakennuslaitos on perustettu vuonna 1994 puolustusministeriön rakennusosastosta ja puolustusvoimien alueellisesta kiinteistöorganisaatiosta (Puolustushallinnon rakennuslaitos 2010). Rakennuslaitos on perinyt noilta ajoilta vahvan turvallisuuskulttuurin, joka näkyy työntekijöiden asenteissa ja viraston toimintaprosesseissa. Henkilöstö on sitoutunut turvallisuustoimintaan ja näkee sen osana viraston laatua. Turvallisuus on sisällytetty osaksi Rakennuslaitoksen arvoja ja laitoksen johto on sitoutunut turvallisuustoimintaan ja sen kehittämiseen.

Rakennuslaitoksen turvallisuustoiminta on kattavaa, mutta sen organisointi ei ole kovin formaalia ja turvallisuuden eri osa-alueet ovat osittain pirstoutuneet. Turvallisuusjohtaminen on ollut melko operatiivista ja toimintaa ei ole suunniteltu pitkällä tähtäimellä, mikä on ollut nähtävissä esim. toimintasuunnitelmien puutteena. Rakennuslaitoksessa on nähty, että turvallisuus pitää sisällyttää toimintaprosessien sisään, eikä pitää erillisenä toimintona joka liimataan tarvittaessa toimintamallin päälle.

Valtionhallinnossa on useita turvallisuushankkeita käynnissä, joten Rakennuslaitoksen turvallisuustoiminta on hyvä virtaviivaistaa ja formalisoida järkevään ja hallittuun muotoon, jonka johtaminen olisi selkeästi organisoitua ja mitattavissa olevaa toimintaa.

2.2 Tutkimuksen tavoitteet

Tutkimustyö on osa kokonaishanketta, jonka tavoitteena on luoda Rakennuslaitokselle kokonaisvaltainen turvallisuudenhallintajärjestelmä ja sovittaa se osaksi viraston normaalia johtamistoimintaa. Järjestelmän tulee kattaa kaikki turvallisuuden osa-alueet.

Tämän tutkimuksen tavoitteena on:

- kartoittaa yleisten turvallisuusjohtamismallien rakenne ja menettelyt
- selvittää Rakennuslaitoksen nykyisen turvallisuustoiminnan keskeiset kehittämiskohteet
- laatia alustava ehdotus Rakennuslaitoksen tulevasta turvallisuusjohtamisjärjestelmästä

2.3 Tutkimuksen rajaukset

Tutkimuksessa käsitellään turvallisuusjohtamisen periaatteita Rakennuslaitoksessa. Turvallisuus käsitteenä kattaa koko yritysturvallisuuden kentän, joka on lähtökohtaisesti jaettu EK:n mallin mukaan kymmeneen eri osa-alueeseen (tuotannon turvallisuus, työturvallisuus, ympäristöturvallisuus, pelastustoiminta, valmiussuunnittelu, tietoturvallisuus, henkilöturvallisuus, toimitilaturvallisuus, ulkomaan toimintojen turvallisuus ja rikosturvallisuus).

Tutkimuksessa ei mennä osa-alueiden yksityiskohtiin kuten esim. tietoturvallisuuteen vaan pysytään yleisluontoisella tasolla, jolloin asioita voidaan tutkia johtamisen ja organisoimisen näkökulmasta.

2.4 Terminologia

Tutkimuksessa käytettävä turvallisuuteen liittyvä terminologia noudattaa valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) laatiman tietoturvasanaston (Valtiovarainministeriö 2008b) suosituksia.

3 TAUSTA JA VIITEKEHYS

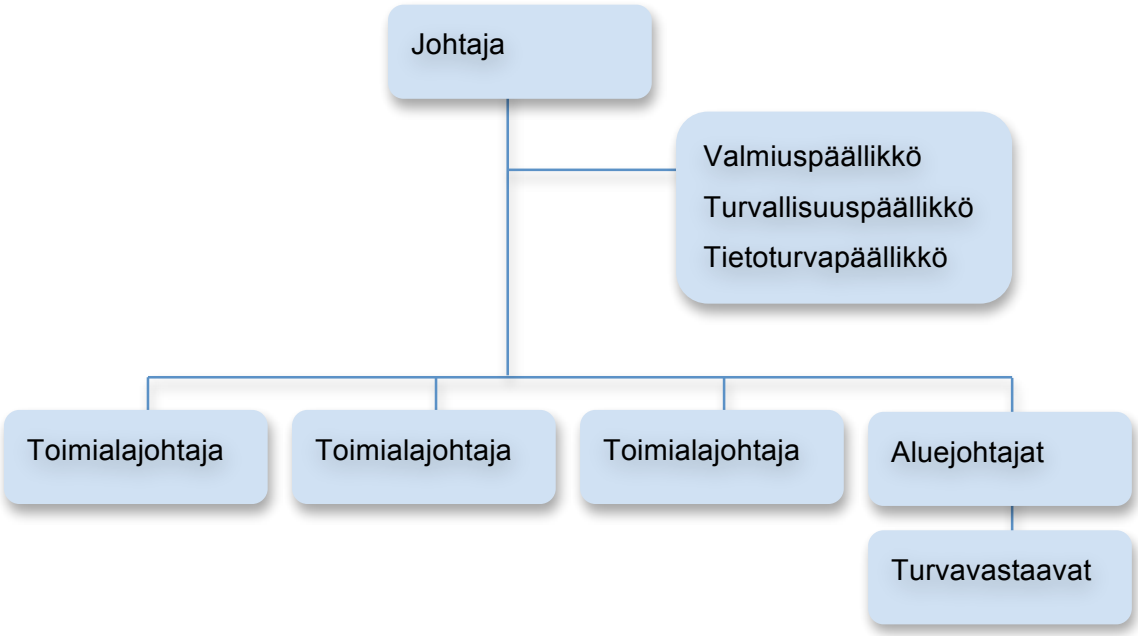
3.1 Puolustushallinnon rakennuslaitos

Puolustushallinnon rakennuslaitos on vuonna 1994 perustettu Puolustusministeriön alainen nettobudjetoitu virasto. Rakennuslaitos vastaa puolustushallinnon kiinteistö- ja ympäristöalan asiantuntija- ja hankintatehtävistä sekä palvelutuotannon järjestämisestä. Virasto hankkii tai tuottaa puolustusvoimille lähinnä asiantuntijatehtäviin, hankesuunnitteluun, varuskuntien kehittämis- ja alueidenkäyttösuunnitteluun, kiinteistönhoitoon, kunnossapitoon, energiahuoltoon, ympäristön suojeluun, tietohallintoon ja erillisiin käyttäjätoimintoihin liittyviä palveluja, joissa on otettu huomioon myös poikkeusolojen valmiusnäkökohdat. Lisäksi Rakennuslaitos tuottaa puolustusvoimille asukasisännöintipalveluja sekä Senaatti-kiinteistöille ja muille puolustusvoimien käytössä olevien tilojen kiinteistövarallisuuden haltijoille rakennuttamis-, omistaja- ja asiantuntijapalveluja. (Puolustushallinnon rakennuslaitos 2009b, s.9.) Laitoksen kokonaisliikevaihto vuonna 2008 oli 141,7 miljoonaa euroa (Puolustushallinnon rakennuslaitos 2009a, s.6). Toimintaa ohjaa mm. asetus Puolustushallinnon rakennuslaitoksesta (18.3.1994/216).

Rakennuslaitos on jakautunut seitsemään alueeseen ja keskusyksikköön. 26 toimipisteessä työskentelee yhteensä 1 002 henkilöä (Valtiokonttori 2010). Toimipisteet ovat hajautuneet ympäri Suomea ja sijaitsevat pääosin varuskuntien yhteydessä. Rakennuslaitoksessa työskentelevien keski-ikä oli lokakuussa 2009 51,48 vuotta. Keski-ikä on huomattavan korkea verrattuna valtion yleiseen tasoon, joka oli vuoden 2009 lokakuussa 43,96 vuotta (Valtiokonttori 2010).

3.1.1 Turvallisuuden organisointi

Rakennuslaitoksen turvallisuutta ohjaavat keskusyksiköstä valmius-, turvallisuus- ja tietoturvapäälliköt. Kokonaisturvallisuuden toteutumisesta vastaa laitoksen johtaja jolle valmius-, turvallisuus- ja tietoturvapäällikkö vastaavat suoraan omasta toiminnastaan. Alueyksiköissä ei ole täyspäiväisiä turvallisuushenkilöitä, vaan turvallisuudesta vastaavat aluejohtajat apunaan toimistokohtaiset oto-työnään toimivat turvallisuus- ja riskienhallintavastaavat.



Kuva 1. Turvallisuuden organisointi Puolustushallinnon rakennuslaitoksessa

Turvallisuutta käsitellään johtoryhmätasolla pysyvänä aiheena, jolle valmiuspäällikkö raportoi kuukausittain laitoksen turvallisuuteen liittyvistä asioista. Lisäksi Rakennuslaitoksessa toimii tietoturvallisuuden johtoryhmä, joka laitoksen ylimpänä turvallisuusinstanssina käsittelee kuusi kertaa vuodessa turvallisuuden kehittämiseen liittyviä asioita.

3.2 Vaatimustenmukaisuus

Lainsäädännön lisäksi Rakennuslaitoksen turvallisuuteen liittyvät normatiiviset tekijät ovat Rakennuslaitoksen ja puolustusvoimien välinen turvallisuussopimus, puolustusministeriön turvallisuustoiminnan strategia sekä kansallinen turvallisuusauditointikriteeristö (KATAKRI), jota vasten puolustusvoimat auditoivat omat sidosryhmänsä.

Puolustusministeriön turvallisuustoiminnan strategia määrittää yleisellä tasolla, mitä asioita Rakennuslaitoksen tulee omassa turvallisuustoiminnassaan huomioida. KATAKRIn vaatimukset menevät huomattavasti tarkemmalle ja käytännönläheisemmälle tasolle.

Asetus Puolustushallinnon rakennuslaitoksesta määrää, että viraston tulee toimia myös poikkeusolojen aikana. Poikkeusolojen toiminta tukeutuu normaaliajan turvallisiin prosesseihin, joten viraston toiminta on lähtökohtaisesti rakennettava turvalliseksi.

3.2.1 Puolustusvoimien turvallisuussopimus

Rakennuslaitoksen pääasiakas on puolustusvoimat, joiden kanssa virastolla on turvallisuussopimus. Sopimuksessa otetaan kantaa yleisellä tasolla turvallisuuden organisoimisesta ja sitoudutaan noudattamaan puolustusvoimien turvallisuusmääräyksiä.

3.2.2 Puolustusministeriön turvallisuustoiminnan strategia

Puolustusministeriön turvallisuustoiminnan strategiassa on linjattu hallinnonalan periaatteet ja järjestelyt. Rakennuslaitoksella ei ole omaa strategiatason turvallisuusasiakirjaa vaan seuraava taso ministeriön strategiasta on Rakennuslaitoksen omat turvallisuuteen liittyvät politiikat kuten riskienhallinta ja tietoturvapolitiikka.

PLM:n turvallisuustoiminnan strategia perustuu Puolustushallinnon strategiseen suunnitelmaan 2025 ja yhteiskunnan elintärkeiden toimintojen strategiaan (Puolustusministeriö 2007).

Strategiassa kuvataan Puolustushallinnon turvallisuustoiminnan päämäärä ja sisältö, nykytila ja päämäärät. Lisäksi strategiassa on kuvataan tulevaisuuden haasteet yleisistä vaatimuksista ja uhkista mahdolliseen Nato-jäsenyyteen.

Puolustushallinnon turvallisuustoiminnan strategian mukaan Rakennuslaitoksen vastuut hallinnonalalla ovat:

- Rakennuslaitoksen turvallisuusohjeistus
- Henkilöstöturvallisuuden toteuttaminen Rakennuslaitoksessa
- Rakennuslaitoksen henkilöstön turvallisuushallinto
- Rakennuslaitoksen tilaturvallisuus
- Rakennuslaitoksen tietoturvallisuus
- Sidosryhmäturvallisuuden toteutus Rakennuslaitoksen hallinnoimissa hankkeissa
- Rakennuslaitoksen materiaaliturvallisuus
- Rakennuslaitoksen ympäristöturvallisuuden toteutus
- Rakennuslaitoksen suojelu- ja pelastustoiminta

PLM:n turvallisuustoiminnan strategiassa mainitaan, että Rakennuslaitoksen turvallisuustoiminnasta vastaa hallintojohtaja apunaan turvallisuuspäällikkö. Asiakirjan laatimisen jälkeen vastuut ovat muuttuneet, jotka korjataan vuoden 2010 aikana julkaistavaan uuteen turvallisuustoiminnan strategiaan.

3.2.3 Kansallinen turvallisuusauditointikriteeristö

KATAKRI valmistui 20.11.2009 osana sisäisen turvallisuuden ohjelmaa. Kriteeristön tarkoituksena on toimia viranomaisten ja yritysten yhteisenä turvallisuuskriteeristönä ja osaltaan yhtenäistää ja parantaa yhteisöturvallisuusmenettelyä, omavalvontaa ja auditointia (Puolustusministeriö 2009). Ennen KATAKRIa Puolustuvoimilla oli oma auditointikriteeristönsä, josta on nyt luovuttu ja siirrytty käyttämään uutta kriteeristöä.

KATAKRI jakaa yritysturvallisuuden neljään osa-alueeseen:

- hallinnollinen turvallisuus
- henkilöstöturvallisuus
- fyysinen turvallisuus
- tietoturvallisuus

Jokainen osa-alue pitää sisällään tietyn määrän kriteereitä, jotka vaihtelevat suojaustason mukaisesti. Tietoturvallisuus pitää sisällään 59 kriteeriä, hallinnollinen turvallisuus 50 kriteeriä, henkilöstöturvallisuus 28 kriteeriä ja fyysinen turvallisuus 27 kriteeriä. KATAKRI on jakanut jokaisen kriteerin eri osiin siten, että suojaustasoille II (korkea taso), III (korotettu taso) ja IV (perustaso) on määritetty organisaatiolta vaadittava vähimmäistaso. Lisäksi kriteeristössä on huomioitu lähtötason suositukset elinkeinoelämän omaehtoista turvallisuustoimintaa varten.

Hallinnollinen turvallisuus tarkastelee turvallisuustyötä turvallisuuden johtamisen ja sen hallintajärjestelmän kannalta. Kriteeristössä ei kuvata kuinka hallintajärjestelmä tulisi rakentaa vaan siinä on kerrottu ne vaatimukset, jotka on otettava huomioon jotta turvallisuuden hallintajärjestelmä olisi vaatimusten mukaisella tasolla. KATAKRI jakaa turvallisuuden johtamisen ja sen hallintajärjestelmän kriteeristön yhdeksään eri osa-alueeseen:

1) turvallisuuspolitiikka
2) turvallisuuden vuotuinen toimintaohjelma
3) turvallisuustyön tavoitteiden määrittely
4) riskien tunnistus, arviointi ja kontrollit
5) turvallisuusorganisaatio ja vastuut
6) onnettomuudet, vaaratilanteet, turvallisuuspoikkeamat ja ennaltaehkäisevät toimenpiteet
7) turvallisuusdokumentaatio ja sen hallinta
8) turvallisuuskoulutus, tietoisuuden lisääminen ja osaaminen
9) raportointi ja johdon katselmukset

Kriteerit vaihtelevat laajuudeltaan melko paljon. Käytännössä KATAKRI antaa vaatimuksia hyvinkin laajoille kokonaisuuksille kuten esim. onko organisaation johto laatinut turvallisuuspolitiikan? Toisaalta KATAKRista löytyy myös kriteerejä, jotka pureutuvat hyvinkin tarkasta käytännön konkretiaan kuten esim. turvallisuuspolitiikan sisältöön.

3.2.4 Jatkuvuuden hallinnan ja tiedon turvaamisen vaatimukset

Jatkuvuuden hallinnan ja tiedon turvaamisen vaatimukset on 15.12.2009 valmistunut kriteeristö ICT-varautumista varten. Vaatimukset ovat osa valtionhallinnon kokonaiskehittämistä sekä yhteiskunnan elintärkeiden toimintojen strategian (YETTS), Valtioneuvoston päätöksen huoltovarmuuden tavoitteista ja valtioneuvoston periaatepäätöksen valtion IT-toimintojen kehittämisestä (Valtion IT-strategia) toimeenpanoa (Valtiovarainministeriö 2006, s.1). Vaatimukset eivät suoraan vaikuta turvallisuuden hallintajärjestelmään, mutta ne antavat vaatimukset suoraan valmiussuunnittelulle ja tietoturvallisuudelle.

Jatkuvuuden hallinnan ja tiedon turvaamisen vaatimukset on jaettu kuudelle eri osa-alueelle:

1) johtajuus
2) strategiat ja toiminnan suunnittelu
3) henkilöstö
4) kumppanuudet ja resurssit
5) prosessit: ICT-jatkuvuuden hallinta
6) mittaaminen

Jokaiselle osa-alueelle on asetettu omat vaatimuksensa, jotka vaihtelevat turvatason mukaan. Vaatimukset tulevat mm. laeista, YETTS:stä, turvallisuusauditointikriteereistä, VAHTI-suosituksista sekä alan yleisistä viitekehyksistä ja standardeista. Vaatimuksissa on määritelty viisi eri tasoa, joiden mukaan organisaation toimintaa säädetään. Kriteeristön tasot ovat:

- lähtötaso
- perustaso
- korotettu taso
- korkea taso
- erityistaso

Lähtötaso on organisaation taso, josta toimintaa lähdetään kehittämään perustasolle. Kehityskulku menee järjestelmällisesti kaikkien tasojen läpi. Normaalitasolta ei voida hypätä suoraan korkealle tasolle.

Perustasolla organisaatio kykenee toimimaan turvallisesti normaalissa, jokapäiväisessä toiminnassaan. Tämä taso on verrattavissa normaalin liikeyrityksen laadukkaaseen toimintaan. Suurin osa valtionhallinnon tietojärjestelmistä on kategorisoitavissa tälle tasolle (Valtiovarainministeriö 2009).

Korotetulle tasolle voidaan sijoittaa organisaation kriittiset toiminnot. Korkeiden vaatimusten takia kaikkia organisaation toimintoja ei ole tarkoituksenmukaista sijoittaa tälle tasolle (Valtiovarainministeriö 2009).

Korkea taso on tarkoitettu YETTS:n erityistilanteiden ja poikkeusolojen varalle. Korkea taso asettaa merkittävät vaatimukset organisaation toiminnalle, joka vaikuttaa myös osaamisvaatimuksiin ja järjestelmien toteutukseen (Valtiovarainministeriö 2009).

Erityistaso on varattu toiminnalle, joka ylittää korkean tason vaatimukset. Näitä vaatimuksia ja toteutuskeinoja hallinnoi kukin hallinnonala itsenäisesti (Valtiovarainministeriö 2009).

ICT-varautumiselle on asetettu seuraavanlainen aikataulu:

Vuoden 2011 loppuun mennessä hallinnonalojen ja virastojen tulee:
kuvata keskeiset toiminta- ja palveluverkostot
määritellä jokaiselle organisaatiolle, palveluille ja järjestelmille tavoitevaatimustaso.
määrittää osaamistarpeet ja aloittaa johdon ja avainhenkilöiden kouluttaminen
määrittää aikataulu, jossa saavutetaan vaatimustasojen mukainen palvelutaso
resursoida käytännön toteutus osana normaalia viraston toimintaa (Valtiovarainministeriö 2009).

Vuoden 2012 loppuun mennessä kriittisimpien palveluiden on oltava vähintään perustasolla. Hankinnoissa ja tarkastustoiminnassa on huomioitava jatkuvuuden hallinta ja tietoturvallisuus (Valtiovarainministeriö 2009).

Vuoden 2016 loppuun mennessä valtionhallinnon kaikki organisaatiot, palvelut ja järjestelmät on oltava niille asetetulla tavoitetasolla (Valtiovarainministeriö 2009).

3.2.5 Valtionhallinnon tietoturvatasot

Tietoturvatasot on kriteeristö, jonka mukaan valtionhallinnon virastojen tulee oma tietoturvallisuutensa järjestää. Tavoitteena on, että jokainen valtion organisaatio täyttää tietoturvallisuuden perustason vuoden 2011 loppuun mennessä. Verkottuneessa toiminnassa perustasoa edellytetään myös palveluiden tuottajilta.

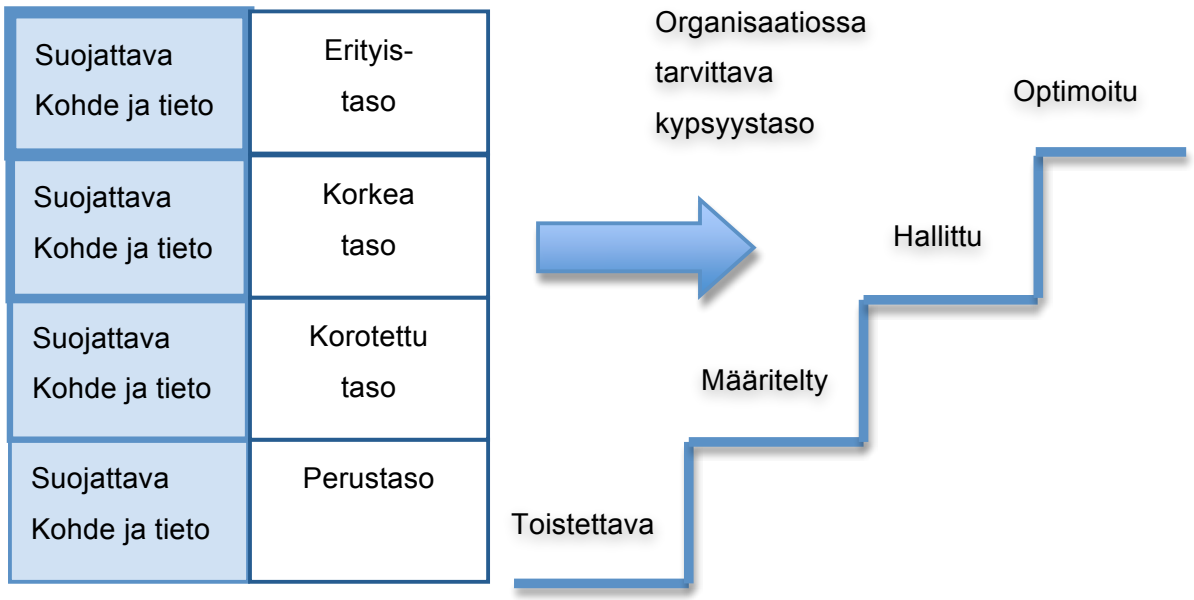
Tietoturvatasot perustuvat yleisesti tunnettuihin standardeihin ja viitekehyksiin, kuten Common Assessment modell CAF, VAHTI-suositukset, Information Management Maturity Model (ISM3), ISO 27001 ja COBIT. Lisäksi tietoturvatasot sopivat yhteen jatkuvuuden hallinnan ja tiedon turvaamisen vaatimusten sekä Huoltovarmuuskeskuksen HUOVIn ja SOPIVAn kanssa.

Tietoturvatasoissa turvallisuus käsitetään turvallisuustasona ja organisaation kypsyytenä. Käsiteltävän tiedon luonne määrää tietoturvatason, jota organisaatiossa ja mahdollisissa alihankintajärjestelyissä on noudatettava. Tietoturvatasot jakaa turvallisuuden neljään eri luokkaan:

1) Perustaso
2) Korotettu taso
3) Korkea taso
4) Erityistaso

Turvallisuuskontrollit ja mekanismit riippuvat turvallisuusluokasta. Tietoturvatasojen mukaan organisaation kykyä ohjata tietoturvatoimintaa mittaa kypsyysajattelu. Perusajatuksena on se, että organisaatiolla tulee olla ohjausmenetelmät ja prosessit tietoturvallisuuden hallintaan. Jos näitä ei ole, ei organisaatio ole riittävän kypsä ohjaamaan tietoturvatoimijoita, eli käytännössä organisaation tietoturva ei vastaa tarvittua tai panostus ei ole kustannustehokasta. Organisaation kypsyyttä mitataan viiden eri tason avulla:

1) Aloittava
2) Toistettava
3) Määritelty
4) Hallittu
5) Optimoitu



Kuva 2. Tietoturvatasot (Valtiovarainministeriö 2008a)

Aloittavalla tasolla organisaation toiminta kyseisen prosessin kohdalla riippuu tekijästä. Käytössä ei ole yhteisiä ohjeita ja toimintamalleja. Tason tulos ei ole tasalaatuista, joten sitä ei voida hallinnossa käyttää. Toistettava taso on tietoturvatasojen perustaso ja samalla valtionhallinnon minimitaso. Tällä tasolla organisaatiossa on yleisesti sovittu käsitys siitä, miten prosessin tulisi toimia. Virheiden määrä saattaa kuitenkin nousta esim. prosessin hoitajan vaihtuessa. Määritetyllä tasolla eli tietoturvatasojen kannalta korotetulla tasolla prosessikuvaus on dokumentoitu ja henkilöstön on koulutettu sen mukaisesti. Prosessin kannalta ei ole väliä kuka sitä hoitaa. Toiminnan laatu ei riipu tekijästä. Tälle tasolle jokaisen organisaation tulisi pyrkiä. Hallitulla eli korkealla tasolla dokumentoitua prosessia mitataan ja samalla seurataan toiminnan laatua. Virheistä pyritään oppimaan ja varmistamaan toiminnan tasainen laatu. Optimoidulla tasolla prosessissa on käytössä parhaat mahdolliset käytännöt ja seurantamenetelmät. Tällä tasolla prosessi optimoi itseään mittaustulosten perusteella (Valtiovarainministeriö 2008a).

4 TURVALLISUUSJOHTAMISEN MALLIT

Kansallinen turvallisuusauditointikriteeristö itsessään jo muokkaa organisaation turvallisuusjohtamista oikeaan suuntaan ja antaa sille tietyn muodon. Tutkimuksen tavoitteena on tarkastella yleisesti tunnettuja turvallisuusjohtamisen malleja ja tutkia kuinka ne soveltuvat Rakennuslaitoksen toimintaympäristöön. Tarkasteltaviksi malleiksi on valittu seuraavat viitekehykset:

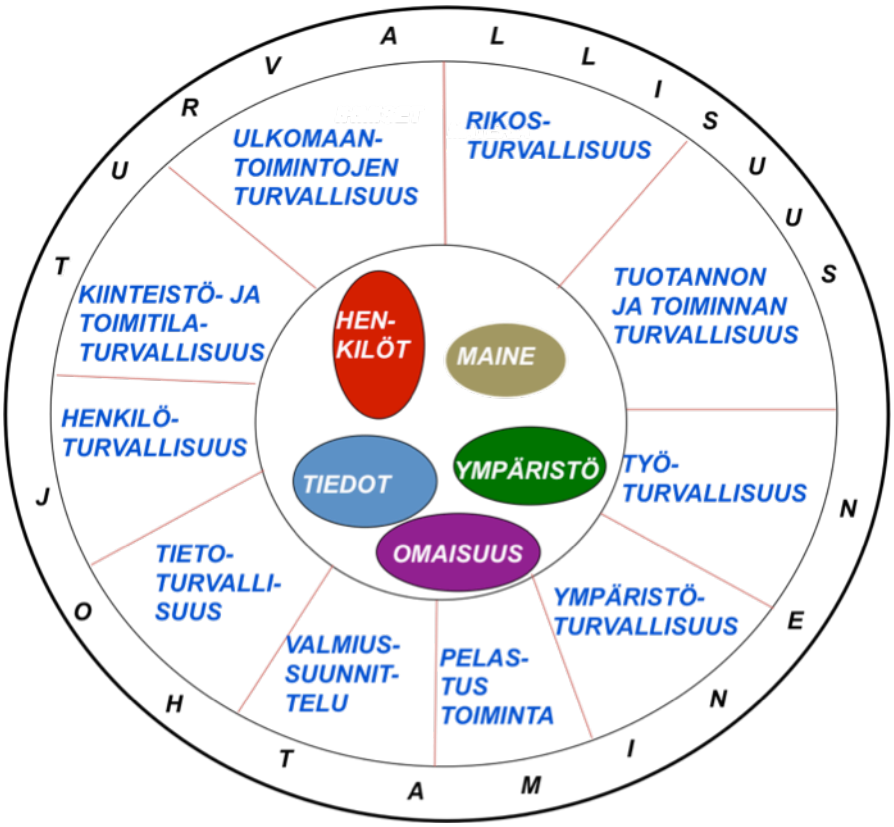
- Yritysturvallisuuden neuvottelukunnan ja Elinkeinoelämän keskusliiton yritysturvallisuuden malli
- OHSAS 18001
- ISO 27001

EK:n yritysturvallisuuden malli on tarkoitettu puhtaasti yritysturvallisuuden kehittämistä varten. OHSAS 18001 on työterveyden- ja työturvallisuudenjohtamisjärjestelmän viitekehys ja ISO 27001 on tietoturvallisuuden hallintajärjestelmän malli.

4.1 Yritysturvallisuus EK

Yritysturvallisuuden neuvottelukunta ja Elinkeinoelämän keskusliitto EK on kehittänyt oman mallin yritysten turvallisuudenhallintaa varten. EK:n mallissa turvallisuustoiminta kuvataan melko yleisellä tasolla. Kovin yksityiskohtaisiin asioihin ei mennä, vaan kerrotaan mistä pitäisi huolehtia ja mitä asioita kuhunkin turvallisuuden osa-alueeseen kuuluu. Tämän tyyppinen lähestymistapa on siitä hyvä, että malli voidaan helposti implementoida organisaation toimintaan. Ongelmana on malliin liittyvien asiakirjojen epämääräisyys ja hajanaisuus. Osa tiedoista kerrotaan selkeästi EK:n extranetissä, mutta osa vain muutamalla lauseella powerpoint-esityksessä.

Turvallisuusjohtamisen tai hallintajärjestelmän rakenteesta mallissa ei oikeastaan puhuta. EK ei myöskään esitä mitään täytettäviä vaatimuksia. Käytännössä mallin implementointi Rakennuslaitokseen tarkoittaa sitä, että laaditaan projektisuunnitelma jossa pyritään mahdollisimman kattavasti huomioimaan jokainen turvallisuuden eri osa-alue. Johtaminen, vastuut, raportointi yms. voidaan sovittaa esim. oman organisaation käytäntöjen mukaiseksi.



Kuva 3. EK:n yritysturvallisuusmalli (Yritysturvallisuus EK Oy 2010)

Kaaviossa sisällä on kuvattu yrityksen arvot, joita yritysturvallisuuden eri funktioilla turvataan. Kaavion ulkokehä kuvaa turvallisuusjohtamista, jolla koko organisaation kokonaisturvallisuutta ohjataan. EK jakaa yritysturvallisuuden kymmeneen eri osa-alueeseen:

1) Tuotannon turvallisuus
2) Työturvallisuus
3) Ympäristöturvallisuus
4) Pelastustoiminta
5) Valmiussuunnittelu
6) Tietoturvallisuus
7) Henkilöturvallisuus
8) Toimitilaturvallisuus
9) Ulkomaan toimintojen turvallisuus
10) Rikosturvallisuus

4.1.1 Tuotannon turvallisuus

Tuotannon turvallisuuden tavoitteena on häiriötön toiminta, nopea toipuminen ja turvalliset tuotteet. Osa-alueen keskeinen sisältö on jatkuvuussuunnittelu, riskien arviointi, tuotevastuu ja turvallisuus, varastointi ja kuljetukset, palvelujen turvallisuus, maksuliikenteen turvallisuus, arvoomaisuuden säilytys, sopimusten turvallisuus, alihankkijat ja toimittajat sekä onnettomuus-, vaara- ja vahinkotilanteiden hallinta (Yritysturvallisuus EK Oy).

4.1.2 Työturvallisuus

Työturvallisuuden tavoitteena on turvallinen työ ja työntekijöiden hyvinvointi. Riskien ennaltaehkäisy ja hyvä yrityskuva. Osa-alueen keskeinen sisältö on työsuojeluvastuun jakaminen, työturvallisuus, koneiden ja työvälineiden turvallisuus, työpaikan sisäinen liikenne, fysikaaliset tekijät, vaarallisten aineiden käsittely, henkilönsuojaimet, väkivallan kohtaaminen työssä, yksintyöskentely ja turvallisuus, työhyvinvointi, työterveyshuolto ja työturvallisuus työpaikalla, jossa toimii useita yrityksiä (Yritysturvallisuus EK Oy).

4.1.3 Ympäristöturvallisuus

Ympäristöturvallisuuden tavoitteena on ekologisen kestävyyden huomiointi, asiakkaiden ja yhteikunnan ympäristöodotusten ennakointi, prosessien ja parhaiden käytäntöjen kehittäminen, vastuun ottaminen ympäristöstä, henkilöstön tietoisuuden lisääminen, avoin tiedottaminen ja sitoutuminen standardien periaatteisiin. Osa-alueen keskeinen sisältö on kestävän kehityksen huomioiminen, ympäristövaikutusten arvioiminen, ilmoitus- ja lupamenettely, vaarallisten aineiden säilytys ja käsittely, ympäristön suojelun hallintajärjestelmä, ympäristön suojelun toimintaohjelma, ilmansuojelu ja päästökauppa, vesien ja maaperän suojelu, meluntorjunta ja maisemansuojelu, kemikaalivalvonta ja jätehuolto (Yritysturvallisuus EK Oy).

4.1.4 Pelastustoiminta

Pelastustoiminnan kohteena on tulipalojen ja muiden onnettomuuksien ennaltaehkäisy ja nopea että oikea vaste onnettomuustilanteissa. Koulutus ja valistustyö. Onnettomuuksiin liittyvä riskienhallinta. Henkilöstön koulutus mm. ensiavun antamiseen ja alkusammutukseen. Osa-alueen keskeinen sisältö on yrityksen varautumis- ja suunnitelmavelvoitteet, pelastussuunnitelma, varautuminen suuronnettomuuksiin, vakuutusyhtiöiden suojeluehdot ja suojeluohjeet, paloturvallisuus, teknillinen turvallisuustaso (mm. alkusammutuskalusto, savunpoisto jne.), tulitöiden turvallisuus ja pelastusalan laitteiden määräaikatarkastukset (Yritysturvallisuus EK Oy).

4.1.5 Valmiussuunnittelu

Valmiussuunnittelun tarkoituksen on turvata yrityksen kriisiajan toiminta. Osa-alueen keskeinen sisältö on varautuminen poikkeusoloihin, tuotannon ja toiminnan suunnittelu, riskiarvioinnin tarkistaminen poikkeusoloihin soveltuvina, energiahuolto, raaka-aineet, koneet ja laitteet, korjaus- ja huoltotoiminta, varaosat, materiaalivarastointi, alihankinta- ja muut palvelutyöt sekä henkilövaraukset (Yritysturvallisuus EK Oy).

4.1.6 Tietoturvallisuus

Tietoturvallisuuden tavoitteena on yrityksen tiedon luottamuksellisuuden, käytettävyyden ja eheyden takaaminen sekä liiketoiminnan jatkuvuuden turvaaminen. Asiakkaan tietojen turvaaminen. Tietoturvallisuuden menetelmien jatkuva seuraaminen ja omien toimenpiteiden jatkuva parantaminen. Osa-alueen keskeinen sisältö on tietojen merkityksen arvioiminen organisaatiolle, tietojen luokittelu ja käsittely eri luottamuksellisuusluokissa, hallinnollinen tietoturvallisuus, tietosuoja, tietotekninen turvallisuus, tietosodankäynti ja tietojärjestelmien toiminnan jatkuvuuden varmistaminen (Yritysturvallisuus EK Oy).

4.1.7 Henkilöturvallisuus

Henkilöturvallisuuden tavoitteena on työntekijöiden suojaaminen rikoksilta ja onnettomuuksilta. Liiketoiminnan suojaaminen estämällä rikollisen aineksen soluttautuminen yritykseen. Avainhenkilöiden suojaaminen. Liiketoiminnalle kriittisten henkilöresurssien varmentaminen. Osa-alueen keskeinen sisältö on asiakkaiden turvallisuus, henkilöstön turvallisuus, kodin ja perheen turvallisuus, matkustusturvallisuus, henkilösuojaus erityistapauksissa, tavoitettavuus- ja hälytysjärjestelmät, varamiesjärjestelyt ja luotettavuusmenettelyt (Yritysturvallisuus EK Oy).

4.1.8 Toimitilaturvallisuus

Toimitilaturvallisuuden tavoitteena on yrityksen keskeisten toimipaikkojen ja -tilojen kustannustehokas suojaaminen. Osa-alueen keskeinen sisältö on toimitilaturvallisuusluokitus, rakenteellinen turvallisuus, turvallisuusvalvonta, kokousten ja neuvottelujen turvallisuus, sopimushallinta ja ulkoistaminen sekä ylläpito ja huoltosopimukset (Yritysturvallisuus EK Oy).

4.1.9 Ulkomaantoimintojen turvallisuus

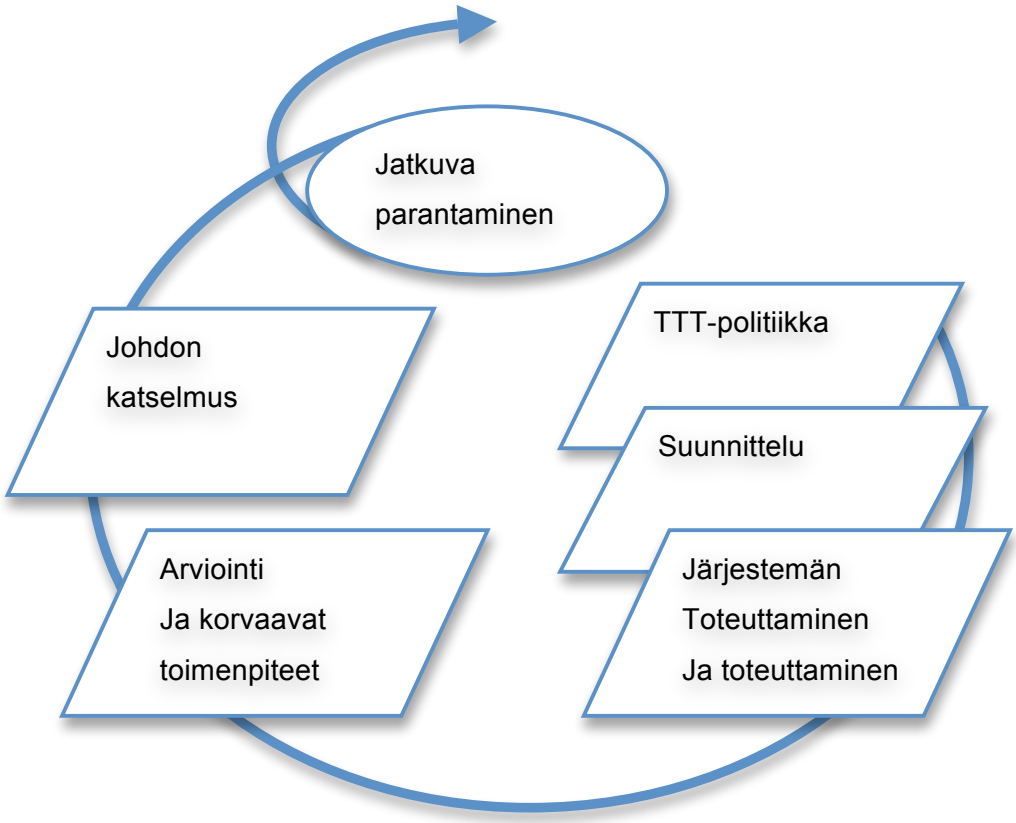
Ulkomaantoimintojen turvallisuudessa keskitytään henkilöstön turvallisuustason takaamiseen heidän ollessa ulkomailla vailla kotimaansa palveluja. Kohdemaan korkean riskitason poistamiseen tai pienentämiseen. Osa-alueen keskeinen sisältö on maiden riskiluokitus, matkustajan status ja yleiset ohjeet (Yritysturvallisuus EK Oy).

4.1.10 Rikosturvallisuus

Rikosturvallisuudella pyritään rikosten ennaltaehkäisyyn ja tapahtuneiden rikosten selvittämiseen sekä rikostilanteen seuraamiseen. Osa-alueen keskeinen sisältö on yrityksen toimintaan, henkilöstöön ja omaisuuteen kohdistuva rikollisuus, rikosriskien hallintakeinot, teknisten laitteiden huolto ja kunnossapito sekä yhteistoiminta viranomaisten kanssa (Yritysturvallisuus EK Oy).

4.2 OHSAS 18001:2007

OHSAS 18001 on työterveyden- ja työturvallisuudenjohtamisjärjestelmän (TTT) viitekehys. Standardin tarkoituksena on antaa organisaatioille tehokkaan TTT-järjestelmän rakenneosat, jotka ovat yhdistettävissä muihin johtamisen tarpeisiin ja edistävät organisaatiota saavuttamaan TTT- ja taloudelliset päämäärät. Standardi perustuu Suunnittele-Toteuta-Arvioi-Toimi (PDCA)-sykliin. Mallin idea on ympyrä jota kierretään: ensin suunnitellaan mitä tehdään, jonka jälkeen toteutetaan suunnitelma. Seuraavaksi arvioidaan toiminta ja lopuksi korjataan havaitut puutteet ja virheet. Kun ympyrä on päästy loppuun palataan taas alkuun, eli toiminnan suunnitteluun (Suomen Standardoimisliitto SFS 2007a).



OHSAS 18001 rakenne (Suomen Standardoimisliitto SFS 2007a)

OHSAS 18001 -standardi koostuu kuudesta vaatimuksesta, jotka organisaation on täytettävä:

1) yleiset vaatimukset
2) TTT-politiikka
3) suunnittelu
4) järjestelmän toteuttaminen ja toiminta
5) tarkastukset ja korjaavat toimenpiteet
6) johdon katselmus

Standardin yleisten vaatimusten mukaan organisaation tulee luoda, dokumentoida ja toteuttaa TTT-järjestelmä ja ylläpitää ja jatkuvasti parantaa sitä OHSAS-standardin vaatimusten mukaisesti sekä määrittää kuinka se täyttää nämä vaatimukset (Suomen Standardoimisliitto SFS 2007a, s. 20).

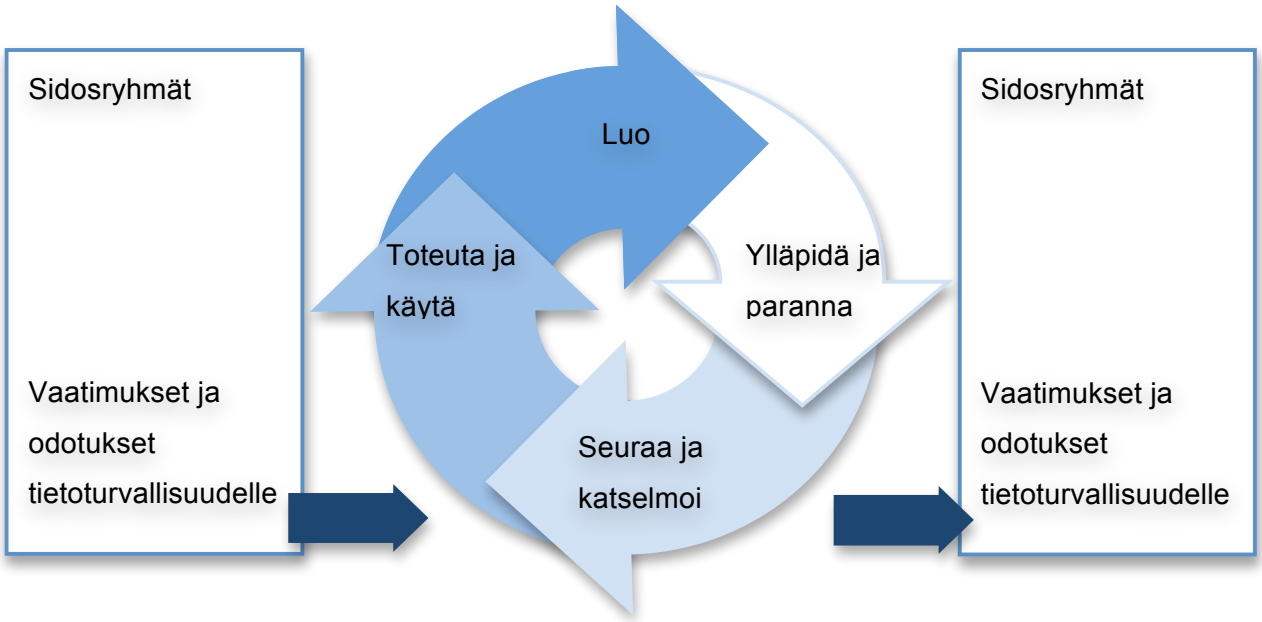
Standardin mukainen politiikka on oltava sidoksissa organisaation TTT-riskien laajuuteen ja luonteeseen. Sen tulee sisältää sitoutuminen vammojen ja terveyden ehkäisemiseen, TTT-toimintojen jatkuvaan parantamiseen sekä vaatimustenmukaisuuden huomioimiseen. Politiikassa on määriteltävä TTT-päämäärät ja katselmoinnin toteutus. Politiikka on dokumentoitava, tiedotettava ja jalkautettava käytäntöön sekä päivitettävä tietyin aikavälein. Lisäksi se on oltava sidosryhmien saatavilla. TTT-suunnittelun on katettava riskienhallinta, vaatimustenmukaisuus sekä päämäärät ja toimintaohjelmat. Riskienarvioinnissa on standardin mukaan huomioitava vaarojen tunnistaminen ja riskianalyysin sekä kontrollien määrittäminen. Analyysit on ulotettava sisäisten riskien lisäksi organisaation ulkopuolisiin uhkiin ja toiminnan muutostenhallintaan. Vaatimustenmukaisuutta on ylläpidettävä siten, että organisaatiolla on olemassa toimintamalli sovellettavissa olevien lakisääteisten ja muiden TTT-vaatimusten tunnistamiseen ja käyttöönottoon. Nämä vaatimukset on oltava ajan tasalla ja tiedotettu organisaation henkilökunnalle. TTT-politiikan lisäksi organisaation tulee ylläpitää dokumentoidut ja mitattavissa olevat TTT-päämäärät asiaankuuluville toiminnoille ja organisaatiotasoille. Päämäärien saavuttamiseksi organisaation on ylläpidettävä TTT-ohjelmia jotka sisältävät vähintään vastuut päämäärien saavuttamisesta ja keinot ja aikataulu, jolla ne saavutetaan (Suomen Standardoimisliitto SFS 2007a).

4.3 ISO 27001

ISO 27001 on tietoturvallisuuden hallintajärjestelmän viitekehys. Hallintajärjestelmä koostuu yhdestätoista eri osa-alueesta:

1) turvallisuuspolitiikka
2) tietoturvallisuuden järjestäminen
3) suojattavien kohteiden hallinta
4) henkilöstöturvallisuus
5) fyysinen turvallisuus ja ympäristön turvallisuus
6) tietoliikenteen ja käyttötoimintojen hallinta
7) pääsyoikeuksien valvonta
8) tietojärjestelmien hankinta, kehitys ja ylläpito
9) tietoturvahäiriöiden hallinta
10) liiketoiminnan jatkuvuuden hallinta
11) vaatimustenmukaisuus

Kuten OHSAS 18001, myös ISO 27001 nojaa PDCA-sykliin.



Kuva 4. ISO 27001 PDCA-sykli (Suomen Standardoimisliitto SFS 2006b)

ISO 27001 -standardin mukaan organisaation tulee luoda, toteuttaa, käyttää, valvoa, katselmoida, ylläpitää ja jatkuvasti kehittää dokumentoitua tietoturvallisuuden hallintajärjestelmää, joka tukee organisaation liiketoimintoja ja organisaatioon kohdistuvia riskejä (Suomen Standardoimisliitto SFS 2006b, s14). Hallintajärjestelmän luominen ja johtaminen on jaettu PDCA-mallin mukaisesti neljään eri osa-alueeseen:

1) Luominen
2) Toteuttaminen
3) Valvonta ja katselmointi
4) Ylläpitäminen ja parantaminen

Hallintajärjestelmän luomisen ISO-standardi jakaa kymmeneen osaan. Prosessissa on määritettävä hallintajärjestelmän kattavuus, tietoturvapolitiikka, riskien arvioinnin toimintatapa, riskien tunnistaminen ja vaikutukset liiketoimintaan sekä riskien käsittelyn vaihtoehdot. Lisäksi hallintajärjestelmässä on kuvattava riskien käsittelyn turvamekanismit, hankkia johdolta hyväksyntä jäännösriskeille ja tietoturvallisuuden hallintajärjestelmän käyttöönotolle ja käytölle sekä laatia toteutussuunnitelma (Suomen Standardoimisliitto SFS 2006b).

Toteutusvaiheessa on määriteltävä ja otettava käyttöön riskienkäsittelysuunnitelma, toteuttaa turvamekanismit ja kontrollit, luotava menettelytapa turvallisuuden mittaamiseen, toteuttaa koulutus ja tietoisuusohjelmat sekä johtaa hallintajärjestelmän käyttötoimintoja ja resursseja (Suomen Standardoimisliitto SFS 2006b).

Hallintajärjestelmän valvonta ja katselmointi on tehtävä siten, että normaalien tietoturvakontrollien lisäksi seurataan turvamekanismien ja hallintajärjestelmän tehokkuutta, katselmoidaan riskien arviointi tietyin väliajoin sekä tarkastetaan jäännösriskin ja hyväksyttävän riskin taso. Lisäksi hallintajärjestelmä on auditoitava tietyin väliajoin joko sisäisen tarkastuksen tai ulkopuolisen tahon toimesta ja varmistua siitä, että hallintajärjestelmän kattavuus on riittävä ja jatkuvan parantamisen kohteet tietoturvaprosessissa on tunnistettu. Turvallisuussuunnitelmia on päivitettävä tarkkailu- ja katselmustoimintojen tulosten mukaan (Suomen Standardoimisliitto SFS 2006b).

Hallintajärjestelmän ylläpitäminen ja parantaminen tapahtuu havaittujen parannustoimenpiteiden pohjalta. Lisäksi organisaation pitää soveltaa sekä oman toisten organisaatioiden tietoturvakokemuksista opittuja asioita sekä varmistaa parannusten lopputulos ja tiedottaa hallintajärjestelmän kehityksestä kaikille sidosryhmille (Suomen Standardoimisliitto SFS 2006b).

5 NYKYTILAN ARVIO

5.1 Turvallisuuskulttuuri

Rakennuslaitoksen turvallisuuskulttuuri on aina ollut korkealla. Tämä johtunee toimialasta ja viraston historiasta. Rakennuslaitos on vuonna 1994 muodostettu puolustusministeriön rakennusosastosta ja puolustusvoimien alueellisesta kiinteistöorganisaatiota, joten työntekijät ovat lähtökohtaisesti sitoutuneet turvallisuustyöhön. Uudet työntekijät ovat omaksuneet kollegoidensa sitoutuneisuuden turvallisuuteen. Työntekijät pitävät turvallisuutta laatutekijänä ja ymmärtävät turvallisuuden merkityksen organisaation toiminnalle. Turvallisuuden mittaamista ei ole vielä otettu Rakennuslaitoksessa käyttöön, joten tarkkoja tietoja henkilöstön sitoutuneisuudesta ei ole saatavilla.

5.2 Hallintajärjestelmä

Turvallisuuden hallintajärjestelmä on Rakennuslaitoksessa verrattain uusi käsite. Turvallisuutta ja sen ohjaamista ei ole täysin formalisoitu, joten tämän hetkisessä tilassa viraston turvallisuudenhallintajärjestelmä on ehkä harhaanjohtava termi. Turvallisuuden ohjaaminen on ollut enemmän käytännöstä lähtevää ja osittain reaktiivista.

Turvallisuutta ohjaavat dokumentit ovat jokseenkin hajallaan ja ongelmana on mm. käytettävä terminologia. Tietoturvallisuudessa puhutaan politiikoista, turvallisuuden ja riskienhallinnan ohjaamisessa strategioista. Ongelmaan on kuitenkin puututtu ja asiakirjoja ollaan paraikaa päivittämässä ja terminologiaa harmonisoimassa yhdenmukaiseksi.

5.2.1 Rakenne

Rakennuslaitoksen turvallisuudessa tietoturvallisuus on hyvin tärkeässä osassa. Vaikka hallintajärjestelmän rakennetta ei virallisesti ole olemassa, on kaikkien turvallisuuden osa-alueiden taustalla tietoturvallisuus.

5.2.2 Politiikat, suunnittelu ja toteutus

Turvallisuutta ohjaavat turvallisuusstrategia ja riskienhallintaa riskienhallintastrategia. Tietoturvallisuutta ohjaavat tietoturva- ja tietosuojapolitiikat. Nämä dokumentit eivät keskenään muodosta mitään hierarkiaa vaan ovat keskenään melko tasavertaisia. Tämä antaa sekavan kuvan turvallisuuden organisoimisesta. Vaihteleva terminologia (politiikka vs. strategia) ei myöskään edesauta turvallisuudenhallintajärjestelmän hahmottamista.

Turvallisuuteen liittyvien toimintojen ja prosessien suunnittelu tapahtuu turvallisuusyksikön sisällä. Seuraavan vuoden kehitystoimenpiteistä sovitaan työntekijän ja esimiehen välisissä tulosneuvotteluissa. Toteutumista seurataan kehityskeskusteluissa ja tietoturvallisuuden johtoryhmässä.

Turvallisuus on pyritty integroimaan osaksi muita prosesseja. Rakennuslaitoksella on käytössä laatujärjestelmä, johon turvallisuus on sisällytetty mukaan. Koulutusta ei ole annettu säännöllisesti ja ohjeiden kattavuus ei ole täydellinen. Käytännössä toimintamallit on jalkautettu koko organisaatioon alueiden turvavastaavien avulla.

5.2.3 Seuranta ja arviointi

Turvallisuuden toteutumista seurataan laitoksen johtoryhmätasolla ja erillisessä tietoturvallisuuden johtoryhmässä. Turvallisuuden ohjaamista ei vielä mitata ja arviointi tapahtuu kvalitatiivisin perustein. Tietoturvapolitiikan mukaan laitoksen tietoturvallisuudesta raportoidaan johtoryhmälle vähintään kerran vuodessa.

5.2.4 Jatkuva parantaminen

Jatkuvan parantaminen perustuu riskianalyyseihin, joiden mukaan toimintaprosesseja kehitetään turvallisemmaksi. Laitoksen johto sopii riskienhallintapalveluiden kanssa tulostavoitteet, joiden mukaan turvallisuuden hallintajärjestelmää kehitetään paremmaksi.

6 TAVOITETILA

6.1 Turvallisuuskulttuuri

Tavoitetilassa Rakennuslaitoksen kaikilla tasoilla omaksuttu jatkuvan parantamisen idea. Kaikki voivat osallistua turvallisuuden parantamiseen helposti lähestyttävän kanavan kautta. Turvallisuuden kehittämisessä kiinnitetään huomioita nykytilaan ja tulevaisuuteen siten, että ongelmakohdat pyritään löytämään proaktiivisesti ja niihin puututaan ennakoivasti. Päätöksiä tehtäessä osataan tunnistaa riskit ja turvallisuusvaikutukset kaikilla tasoilla. Virheitä pyritään tarkastelemaan työprosessien kannalta siten, että ymmärretään miksi virhe tai vaaratilanne tapahtui.

6.2 Hallintajärjestelmä

6.2.1 Rakenne

Turvallisuudenhallintajärjestelmässä on huomioitava kaikki turvallisuuden eri osa-alueet ja sen on perustuttava PDCA-mallin mukaiseen jatkuvaan kehitykseen. Järjestelmässä on huomioitava ulkopuoliset vaatimukset, riskianalyysien tulokset ja suojattavat kohteet. Hallintajärjestelmä ei saa olla liian jäykkä vaan sen on oltava skaalautuva ja Rakennuslaitoksen tarpeisiin mukautuva.

6.2.2 Politiikat, suunnittelu ja toteutus

Turvallisuutta ohjaavat asiakirjat on oltava selkeitä ja ajan tasalla. Politiikat katselmoidaan tietyin aikavälein ja mahdolliset muutokset jalkautetaan ja tiedotetaan henkilökunnalle. Suunnittelun on oltava johdonmukaista ja siinä on huomioitavat riskianalyysien, kontrollien ja mittareiden tulokset. Käytännön toteutusta ohjaa aina sitä varten laadittu toteutussuunnitelma.

6.2.3 Seuranta ja arviointi

Rakennuslaitoksen turvallisuuden tilaa arvioidaan riskianalyysien, kontrollien, mittareiden, henkilöstön kehittämisideoiden, poikkeamien ja harjoitusten avulla. Tulokset viedään käytäntöön toimintasuunnitelmien avulla. Turvallisuuden tilasta raportoidaan laitoksen johdolle ennalta määritetyn mallin mukaisesti.

6.2.4 Jatkuva parantaminen

Turvallisuuden kehitys tapahtuu PDCA-mallin mukaisesti, joka on viety käytäntöön esim. turvallisuuden vuosikellon avulla. Toimintaa kehitetään seurannan ja arvioinnin pohjalta siten, että resurssit osataan kohdistaa oikeisiin kohteisiin.

7 NYKYTILAN KEHITTÄMISAJATUKSIA

7.1 Turvallisuudenhallintajärjestelmä

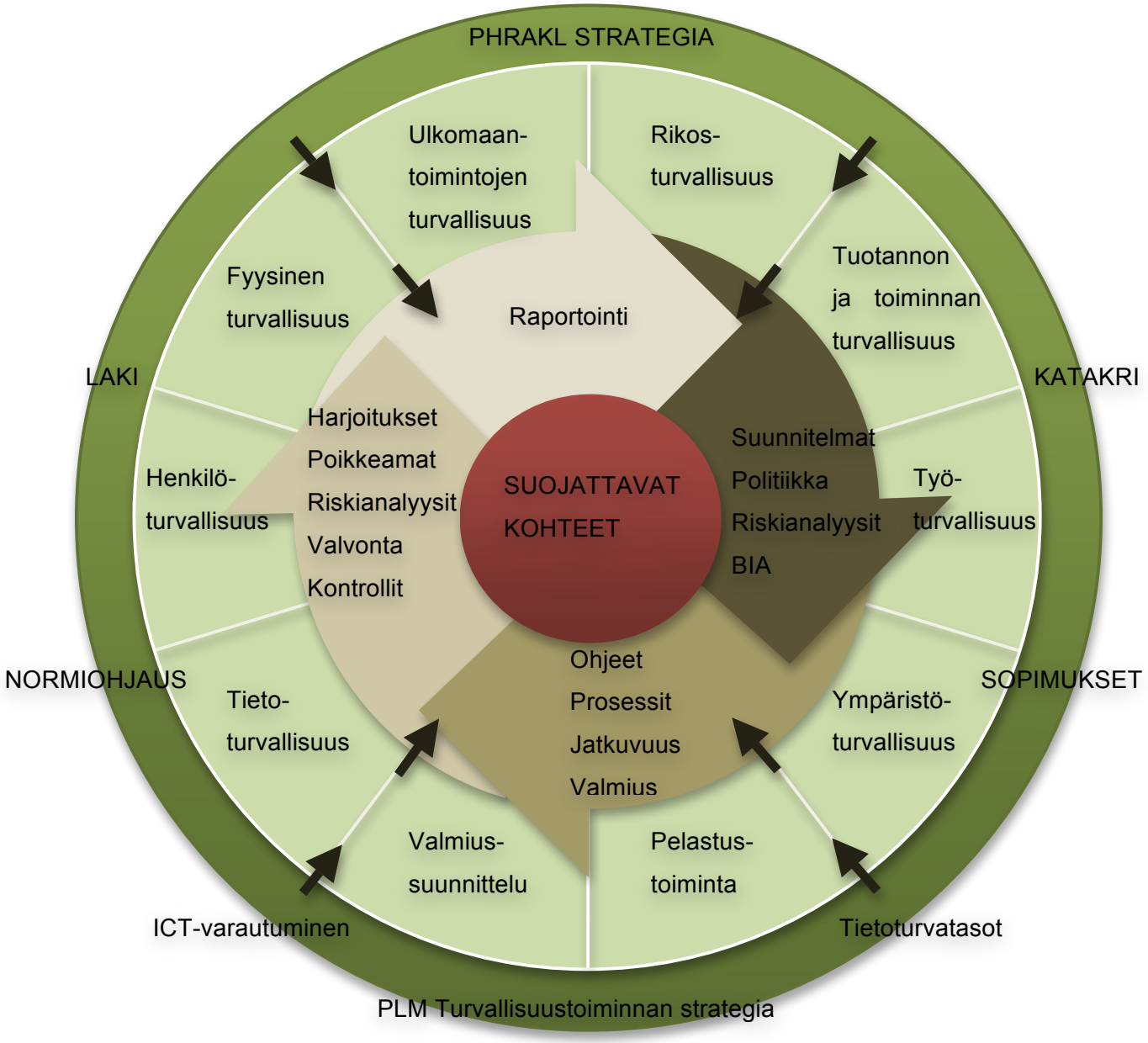
Valmiit mallit kuten OHSAS 18001, ISO 27001 tai EK:n malli ei sellaisenaan sovellus Rakennuslaitoksen käyttöön. EK kertoo mitä osa-alueita turvallisuuden hallinnassa tulee ottaa huomioon, mutta hallintajärjestelmän rakenne ei huomioi PDCA-mallia tai organisaation turvallisuuteen vaikuttavia tekijöitä, kuten laki ja sopimukset. ISO 27001 ja OHSAS 18001 antaa kattavan kuvan rakenteesta, mutta kummassakaan mallissa ei huomioida yritysturvallisuuden kaikkia osa-alueita.

Rakennuslaitoksen kannalta parhaaseen lopputulokseen päästään, jos valmiista malleista yhdistetään yksi kokonaisuus. Turvallisuuden hallintajärjestelmässä on huomioitava ulkopuoliset vaatimukset kuten laki, sopimukset ja turvallisuuskriteeristöt. Nämä vaikuttavat yhdessä turvallisuuden eri osa-alueille, jotka on johdettu EK:n mallista. Tähän malliin lisäämällä PDCA-sykli saadaan hyvä ja yksinkertainen kokonaisuus, joka palvelee parhaiten Rakennuslaitoksen tarpeita. Viemällä turvallisuuden osa-alueet PDCA-sykliin, saadaan kokonaisuus joka on suunniteltua ja kattavaa, sisältää tarpeelliset kontrollit ja kokonaisuudesta raportoidaan organisaation johdolle. ISO 27001 mukaisen tietoturvallisuuden hallintajärjestelmä toimii sellaisenaan kokonaisturvallisuuden hallinnassa. Mallin vaatimukset hallintajärjestelmälle on hyvin yleisluontoiset, joten ne on helposti johdettavissa laajempaan kontekstiin.

ISO 27001-mallin implementoiminen kokonaisturvallisuuden hallintajärjestelmäksi mahdollistaisi tietoturvallisuuden ja kokonaisturvallisuuden hallintajärjestelmien yhdistämisen. Tämä selkeyttäisi dokumentaatiota ja johtamistapoja. Rakennuslaitokselle asetetut ulkopuoliset turvallisuuskriteeristöt sopivat sellaisenaan ISO 27001 mallin rakenteeseen.

Kuvassa 5 on kuvattu malli Rakennuslaitoksen turvallisuudenhallintajärjestelmäksi. Ulommaisella kehällä on ulkopuoliset vaatimukset kuten Puolustusministeriön turvallisuustoiminnan strategia, joka omalta osaltaan antaa vaatimuksia mm. turvallisuuden eri osa-alueille. Seuraavalla kehällä on kuvattu turvallisuuden eri osa-alueet, jotka on huomioitava PDCA-syklin mukaisessa prosessissa. Jokaisen turvallisuuden osa-alue on käytävä sama prosessi läpi, eli riskianalyysien pohjalta tehdään turvallisuuspolitiikka ja toimintasuunnitelmat, jotka jalkautetaan käytäntöön ohjeiden ja prosessien kautta. Toimintaa seurataan ja mitataan mm. kontrollien ja poikkeamien

kautta. Tulokset raportoidaan johdolle, jonka jälkeen palataan takaisin alkuun, eli suunnitelmien laatimiseen. Keskimmäisenä kuvassa on suojattavat kohteet kuten henkilöstö, tieto ja maine.



Kuva 5. Puolustushallinnon rakennuslaitoksen turvallisuudenhallintajärjestelmä

7.2 Keskeiset kehittämistarpeet

Turvallisuusjohtamisjärjestelmän formalisointi on itsessään lähtökohta toimivalle turvallisuusjohtamiselle. Roolien selkeyttäminen on turvallisuuden ja toiminnan tehokkuuden kannalta olennainen asia.

Johtamisjärjestelmän osa-alueet ja niiden toimintapolitiikat on päivitettävä ja kehitettävä ajantasalle. Turvallisuuden terminologia on harmonisoitava, jotta kokonaiskuva on selkeä myös linjaorganisaatiolle. Turvallisuuspolitiikka ja käytännöt on laadittava siten, että ne kattavat kaikki turvallisuuden osa-alueet.

Suunnitelmallisuus, kontrollit ja raportointi ovat avainasemassa turvallisuuden kehittämisessä. PDCA-syklin sisällyttäminen kaikkeen turvallisuustoimintaan takaa formaalin ja kattavan prosessin. Käytännössä esim. turvallisuustoiminnan vuosikello varmistaisi PDCA-syklin.

Turvallisuuden hallinnalle ja johtamiselle asetetut ulkoiset vaatimukset, kuten turvallisuuspolitiikan laatiminen, sisältö, päivittäminen yms. asiat tulisi kirjata Rakennuslaitoksen laatujärjestelmään omiksi prosesseiksi. Tällä toimenpiteellä turvallisuuden johtaminen saataisiin sisäisen valvonnan piiriin.

Tietoturvallisuuden hallintajärjestelmä ja turvallisuuden hallintajärjestelmä voidaan yhdistää, jolloin toiminta yksinkertaistuu ja on paremmin hallittavissa. Tämä onnistuu, jos turvallisuuden hallintajärjestelmän rakenne kehitetään ISO 27001 -standardin pohjalta. Tietoturvallisuus nähdään kuitenkin osana kokonaisturvallisuutta, joten erillistä hallintajärjestelmää ei kannata rakentaa.

Turvallisuusasiakirjojen hierarkiaa on kevennettävä siten, että Rakennuslaitoksessa pyrittäisiin yhteen politiikkatason asiakirjaan, jossa linjataan yleisellä tasolla kokonaisturvallisuus. Seuraava taso politiikasta on turvallisuuskäytännöt ja alimmalla tasolla käytännön ohjeet. Iso hierarkia vain sekoittaa loppukäyttäjää ja vaikeuttaa ohjeiden löytämistä.

8 YHTEENVETO

Rakennuslaitoksen turvallisuudenhallintajärjestelmän malliksi ei voida ottaa vain yhtä standardia tai viitekehystä. Kokonaisvaltaisen turvallisuuden hallinnan kannalta paras vaihtoehto on yhdistää kaikki mallit ja rakentaa niistä oma järjestelmän. EK:n mallissa on kattavasti huomioitu kaikki turvallisuuden osa-alueet, mutta mallissa ei ole kovin kattavasti kerrottu hallintajärjestelmän rakennetta. OHSAS 18001 ja ISO 27001 ovat rakenteeltaan hyviä, mutta ne eivät ole tarpeeksi kattavia kokonaisturvallisuuden kannalta. Yhdistämällä nämä mallit saadaan järjestelmä, joka kattaa kaikki turvallisuuden osa-alueet ja huomioi myös PDCA-syklin, raportoinnin, kontrollit yms. yleiset hyvään johtamiseen ja hallintoon liittyvät seikat. Valtionhallinnon tietoturvatasoissa, KATAKRIssa ja jatkuvuuden hallinnan ja tiedon turvaamisen vaatimuksissa on hyödynnetty mm. ISO 27001 -standardia, jolloin kaikki nämä kriteerit sopeutuu luonnollisesti yhdistettyyn malliin.

Turvallisuuden hallintajärjestelmän keskeisiä kehittämiskohteita ovat mm. turvallisuusvaatimusten vieminen Rakennuslaitoksen laatujärjestelmään, jolloin ne ovat sisäisen tarkastuksen auditoitavissa. Rakennuslaitoksen turvallisuuteen liittyvien asiakirjojen rakennetta pitäisi keventää siten, että olemassa olevista politiikoista tehdään yksi kaikki turvallisuusalueet kattava politiikka jossa viitataan turvallisuuskäytäntöihin ja toimintamalleihin. Haasteena tässä on politiikan pitäminen tarpeeksi lyhyenä ja selkeänä. Tietoturvallisuuden hallintajärjestelmä ja turvallisuuden hallintajärjestelmä voidaan yhdistää, joka selkeyttää turvallisuuden johtamista ja integroi tietoturvallisuuden kiinteämmin osaksi kokonaisturvallisuutta.

Turvallisuustoiminnan johtamisessa suunnitelmallisuus, kontrollit ja valvonta sekä raportointi ovat avainasemassa. Suunnittele-toteuta-arvio-toimi -syklin sisällyttäminen kaikkeen turvallisuustoimintaan takaa kattavan ja formaalin turvallisuudenhallintajärjestelmän.

LÄHDELUETTELO

Puolustushallinnon rakennuslaitos. 2009a. Henkilöstötilinpäätös 2008. [Viitattu 23.2.2010]. Saatavissa: http://www.phrakl.fi/phrakl/mm.nsf/lupgraphics/henkil%C3%B6st%C3%B6tilinp%C3%A4%C3%A4t%C3%B6s_2008.pdf/$file/henkil%C3%B6st%C3%B6tilinp%C3%A4%C3%A4t%C3%B6s_2008.pdf

Puolustushallinnon rakennuslaitos. 2009b. Toimintakertomus 2008. [Viitattu 23.2.2010]. Saatavissa: http://www.phrakl.fi/phrakl/mm.nsf/lupgraphics/toimintakertomus_2008.pdf/$file/toimintakertomus_2008.pdf

Puolustushallinnon rakennuslaitos. 2010. Puolustushallinnon rakennuslaitoksen historia. [Viitattu 19.2.2010]. Saatavissa: http://www.phrakl.fi/phrakl/Publish.nsf/$all/449DDA4AAB7860C1C2256FC70048EAA7

Puolustusministeriö. 2007. Puolustusministeriön turvallisuustoiminnan strategia. ISBN: 978-951-25-1768-8. Kirjapaino Keili Oy. Saatavissa: www.defmin.fi/files/1093/turvallisuustoiminta-strategia.pdf

Puolustusministeriö. 2009. Kansallinen turvallisuusauditointikriteeristö. ISBN: 978-951-25-2077-0. Saatavissa: http://www.defmin.fi/files/1525/Katakri.pdf

Suomen Standardoimisliitto SFS. 2006b. ISO/IEC 27001:fi. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset

Suomen Standardoimisliitto SFS. 2007a. OHSAS 18001:fi. Työterveys- ja turvallisuusjohtamisjärjestelmät. Vaatimukset

Valtiokonttori. 2010. Netra, valtionhallinnon internetraportointi. Henkilöstöraportointi. [Viitattu 23.2.2010]
Saatavissa: http://www.netra.fi/

Valtiovarainministeriö. 2006. Valtionhallinnon ICT-varautumisen kehittämishanke. Asettamispäätös.
Saatavissa:
http://www.hare.vn.fi/upload/Asiakirjat/15182/134841_Asettamisp%C3%A4%C3%A4t%C3%B6s115042006.pdf

Valtiovarainministeriö. 2008a. Tietoturvatasot käsikirja. Luonnos.
Saatavissa:
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20081103Lausun/02_TTT-kaesikirja-20081029.pdf

Valtiovarainministeriö. 2008b. Valtionhallinnon tietoturvasanasto. ISBN 978-951-804-888-9.
Saatavissa:
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20081211Valtio/Vahti_8_NETTI%2b_KANNET.pdf

Valtiovarainministeriö. 2009. Valtionhallinnon ICT-varautuminen. Jatkuvuuden hallinnan ja tiedon turvaamisen vaatimukset.
Saatavissa:
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/04_hallinnon_kehittaminen/20081113Valtio/ICT-varautuminen_NETTI_%2b_KANNET.pdf

Yritysturvallisuus EK Oy. 2010. Yritysturvallisuus EK:n Extra -palvelu. [Viitattu 23.2.2010]
Saatavissa:
http://www.ek.fi/